

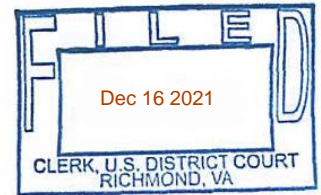
IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF

THE PREMISES LOCATED AT
1600 WESTOVER HILLS BLVD,
RICHMOND, VIRGINIA 23225

Case No. 3:21sw219

FILED UNDER SEAL



**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Alexandra Davila, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the premises located at 1600 Westover Hills Blvd, Richmond, Virginia 23225 (hereinafter referred to as “PREMISES”) as further described in Attachment A, and for the items further described in Attachment B.

2. I, Alexandra Davila, has been a sworn City of Richmond Police Officer for seven years. I have spent approximately five of those seven years assigned to various special investigative units as well as the detective division. I am currently assigned as a detective to Computer Crimes Unit as well as the Internet Crimes Against Children (ICAC) Task Force for Southern Virginia and the Federal Bureau of Investigation (FBI) Child Exploitation Task Force (CETF). I have participated in the preparation and execution of numerous arrest and search warrants for criminal offenses involving violations of the criminal code of Virginia as well as United States Code. I have attended an ICAC Task Force school specifically designed for investigators to understand and conduct investigations related to child pornography. As a task

force officer, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252A (Distribution, Receipt, and Possession of Child Pornography), and 2422(b) (Attempted Coercion and Enticement of a Minor) are located on the PREMISES described in Attachment A. There is also probable cause to search the PREMISES described in Attachment A for evidence and instrumentalities of these crimes further described in Attachment B.

RELEVANT STATUTORY PROVISIONS

5. **Production of Child Pornography:** 18 U.S.C. § 2251(a) provides that it is unlawful for any person to persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct. Subsection 2251(b) further specifies that it is unlawful for any parent, legal guardian, or person having custody or control of a minor to knowingly permit such minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

6. **Distribution or Receipt of Child Pornography:** 18 U.S.C. § 2252A(a)(2) provides that it is a crime to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign

commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. **Possession of Child Pornography:** 18 U.S.C. § 2252A(a)(5) provides that it is a crime to knowingly possess, or knowingly access with intent to view, any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. **Coercion and Enticement:** 18 U.S.C. § 2422(b) provides that it is unlawful for any person, using the mail or any facility or means of interstate or foreign commerce, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

9. **Child pornography or Child abusive material** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexual explicit conduct. *See* 18 U.S.C. § 2256(8).

10. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

11. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).
12. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:
- a. **Computer**, as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
 - b. **Storage medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
 - c. **Wireless telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
 - d. **Smartphone**: A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement),

have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as “apps.” Smartphones can access the Internet through cellular as well as Wi-Fi (“wireless fidelity”) networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

- e. **SIM card:** Stands for a “subscriber identity module” or “subscriber identification module,” which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone’s international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.
- f. **Log Files:** Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- g. **Internet:** A global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- h. **Internet Protocol Address (IP address):** A unique number used by a computer to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- i. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting),

photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMC’s”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage devices).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). As referenced below in the discussion of computer forensics, the term “computer” also refers to smartphones as defined above. While there are differences in aspects of the operational design and associated forensic process to be used for traditional computers like laptops and desktops as compared to smartphones, there are also broad similarities. Use of the generic term “computer” for both categories of devices in a discussion of the computer forensic process is therefore appropriate.

15. **Probable cause.** I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or

years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

16. **Forensic evidence.** As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable

cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “**who, what, why, when, where, and how**” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion.
 - i. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations,

internet history, and anti-virus, spyware, and malware detection programs) can indicate **who** has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner.

- ii. Further, computer and storage media activity can indicate **how** and **when** the computer or storage media was accessed, used and/or created. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.
- iii. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location, i.e., the **where**, of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital

camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user.

- iv. Lastly, information stored within a computer may provide relevant insight into the computer user's state of mind, i.e., the **why**, as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. **Necessity of seizing or copying entire computers or storage media.** In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. **Nature of examination.** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices including cellular telephones consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

19. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

PROBABLE CAUSE

20. On August 30, 2021, your affiant, while acting in an official capacity as a detective with the Richmond Police Department, received a report from the National Center for Missing and Exploited Children (NCMEC) regarding the Twitter account associated with

username "**Pig83god**," ESP User ID 1363425091229466626. The report indicated **Pig83god**, who appeared to be an adult based on information contained in the Twitter user profile, used Twitter to communicate and exchange sexually explicit material with an alleged minor. Additionally, the report contained copies of the preserved files from the **Pig83god**'s Twitter account.

21. Upon review of these files, your affiant identified an exchange of media and messages between **Pig83god** and Twitter user "BuyMeShitLmao," beginning on June 4, 2021, at 08:18:54 UTC. BuyMeShitLmao appeared to be a female approximately 12 years old based on information contained in the Twitter user profile that stated "bi/cis girl IM 12." During the conversation, the following exchange occurred:

Pig83god: hiii
Ur cuteee
Can I send u a video I made for uuu

BuyMeShitLmao: Sure!!

Pig83god then sent a video of what appeared to be an adult male sitting in a chair, masturbating in front of the camera. The male, whose face is visible in the video, can be further described as a white with dirty blonde/brown hair, wearing a black long-sleeved shirt. After sending the video, **Pig83god** requested BuyMeShitLmao send a video in return:

Pig83god: I have one moreee
If youd like to see it!!!

BuyMeShitLmao: Ofccc

Pig83god: oki oki but first
Can I see some of uuu

BuyMeShitLmao: perhaps

Pig83god: ur so hot

BuyMeShitLmao then sent an image of what appeared to be a minor female lying on a bed with a pink shirt on. The female was nude from the waist down and exposed her vagina to the camera. The image appeared to be that of a prepubescent female minor to indicate that this was an image of “BuyMeShitLmao.” Upon receiving the image, **Pig83god** sent another video of the same adult male individual masturbating in front of the camera. Additionally, **Pig83god** stated “omgggg I want to be inside youuuuu.”

22. Later in the conversation, the following exchange occurred:

Pig83god: I wanna see you touch yourself
Show daddy and ill give you a sweet treat
I wanna hear u moan tooo

BuyMeShitLmao then sent a video of what appeared to be a pubescent female minor who exposes her vagina to the camera and digitally manipulates it. The female is wearing a pink and shirt and lying on the bed and is nude from the waist down.

Pig83god: ur so cute!!! Wtf

BuyMeShitLmao: I don’t think I have any moaning videos but
BuyMeShitLmao then sent a video that depicts a female having vaginal intercourse with a dildo. The female has on a long sleeve top and is nude from the waist down. It is unknown who the female is in the video although the conversation alluded to it being the user “BuyMeShitLmao.”

Pig83god: omggg that so hottt

Pig83god then sent another video of what appeared to be a white male lying on a bed fully nude, masturbating. The male’s face is not visible in the video.

23. Upon further review of the information contained in the NCMEC report, agents identified several additional video files which were shared by **Pig83god** via Twitter and contained what appeared to be child pornography. For example:

- i. “1401701096280793092VPIKUrOXj8_abeW_5HJjcgWVOjypcI5_hg16b3Xr8As.mp4” is a color video depicting what appears to be a clothed female minor performing fellatio on an adult male. Based on my training and experience, the girl appears to be approximately 9 to 11 years old. The basis for my conclusion is the youthful appearance of her face, the relatively small size of her hands, which are visible in the video, and the fact that she does not appear to have developed breasts because her shirt lays flat on her chest.
- ii. “1401701100445745157-v3mcH6j5oXcTMDS1BcluuD1CjvoNNyeBvAYvxJEh_8.mp4” is a color video depicting a nude minor female lying on her stomach on a bed while an adult male has vaginal intercourse with her. Given the apparent very small stature of the female, based on training and experience it would appear that she is between 6 to 9 years old.

24. Additionally, the NCMEC report indicated that London Metro Police previously investigated **Pig83god** for another matter wherein **Pig83god** attempted to solicit explicit images and videos from another Twitter user who was confirmed to be approximately 14 years old.

25. The NCMEC report provided multiple logins from the suspect account to include the IP address they used to login along with a date and time. On June 23, 2021, at 05:50:28 UTC, the suspect account was accessed via login IP 174.206.98.224. Open-source research indicated that IP address 174.206.98.224 was registered by Verizon Wireless. On June 24, 2021, at 05:26:26 UTC, the suspect account was accessed via login IP address 72.84.209.156. Open-source research indicated that IP address 72.84.209.156 was registered by Verizon.

26. Pursuant to an administrative subpoena served on Verizon Wireless on August 30, 2021, IP address 174.206.98.224 on June 23, 2021, at 05:50:28 UTC was shown as a “natting” IP¹ with 180 possible phone numbers. The report provided contains all the mobile numbers that utilized the IP(s) during the timeframe requested.

27. Pursuant to an administrative subpoena served on August 30, 2021, to Verizon, the subscriber information associated with IP address 72.84.209.156 on June 24, 2021, at 05:26:26 UTC was listed as Mary Boyes, with an address of the PREMISES.

28. Queries of open source and law enforcement databases indicated the PREMISES is owned by Mary Boyes and another individual named Dennis Rodriguez. Additionally, HENRY BLANCETT (hereinafter SUBJECT), is listed as residing at the PREMISES.

29. Based on records from the Virginia Department of Motor Vehicles, the information contained on the SUBJECT’s driver’s license corresponds to the PREMISES. Upon reviewing the image of the SUBJECT on his driver’s license, agents identified him as the male individual who appears in the videos **Pig83god** sent to BuyMeShitLmao on Twitter.

30. Open-source search of the SUBJECT’s phone number showed the listed number of 804-517-5572. Records provided by Verizon Wireless showed that the SUBJECT’s phone number was included among the phone numbers that utilized the natting IP of 174.206.98.224 on June 23, 2021, at 05:50:28 UTC.

¹ “Natting” derives from the acronym “NAT,” which stands for network address translation. The most common usage of this expression relates to multiple devices on a network sharing the same public-facing IP address. A simple example of natting occurs in households where multiple devices like mobile phones and computers all connect to the Internet through one IP address provided by a residential broadband service. With mobile phone carriers like Verizon, the number of IP addresses that are assigned to the carrier for its use is typically far fewer than the number of unique devices that are attempting to connect to the Internet through the carrier’s network. Thus many mobile phones will connect to the Internet at the same time using the same shared IP address.

31. On September 15, 2021, your affiant and other agents from the FBI Richmond Field Office opened a federal case regarding the matter.

32. A search warrant was executed for the Twitter account of “**Pig83god**” on September 14, 2021. Twitter was able to send the search warrant return via FedEx on a disc by October 7, 2021. Your affiant reviewed the search warrant return which confirmed all the information that had been included in the original CyberTip.

33. During surveillance of the PREMISES conducted on November 1, 2021, law enforcement observed the SUBJECT depart the PREMISES in a blue Honda Pilot bearing license plate VKJ-7167. The SUBJECT exited the PREMISES wearing a black T-Shirt, black jeans, and sneakers and carrying a backpack. The SUBJECT drove to campus at the University of Mary Washington located in Fredericksburg, Virginia, exited the vehicle, and entered one of the residence halls.

34. Your affiant spoke with representatives from the University of Mary Washington who confirmed BLANCETT is currently enrolled at the university and resides in a dormitory on campus. Representatives also advised the semester ends on December 11, 2021, at which time all students must vacate on-campus housing until classes resume in January 2022.

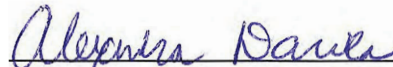
35. Surveillance was done again on the PREMISES on December 13, 2021, at 1345 hours and again on December 14, 2021, at 0730 hours. The blue Honda Pilot bearing license plate VKJ-7167 was observed parked on the side street next to the PREMISES.

CONCLUSION

36. Based on the forgoing, I submit there is probable cause for a warrant to search the PREMISES described in Attachment A for evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252A (Distribution, Receipt, and

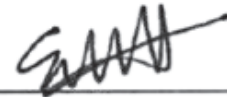
Possession of Child Pornography), and 2422(b) (Attempted Coercion and Enticement of a Minor), as further described in Attachment B.

Respectfully submitted,



Alexandra Davila
Task Force Officer
FBI Richmond Field Office
Child Exploitation Task Force

Attested to by the Affiant by telephone in accordance with the requirements of
FED. R. CRIM. P. 4.1 on this date December 16, 2021


/s/

Elizabeth W. Hanes
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The premises to be searched, known as **1600 Westover Hills Blvd, Richmond, Virginia 23225** in the Eastern District of Virginia, is further described as a one-story residential structure with a second-floor addition and a brick exterior. The main entrance to the home appears on the side of the structure facing Westover Hills Blvd. There appears to be a sidewalk leading up to the main entrance and a detached garage at the back of the property. The premises to be searched includes the entire property. Photos of the premises to be searched are below.



ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. §§ 2251(a) (Production of Child Pornography), 2252A (Distribution, Receipt, and Possession of Child Pornography), and 2422(b) (Attempted Coercion and Enticement of a Minor), including:
 - a. Any and all visual depictions of minors;
 - b. Any and all address books, names and lists of names and addresses of minors;
 - c. Any and all records reflecting physical contacts, whether real or imagined, with minors; and
 - d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
2. Computers, electronic devices, or storage media used as a means to commit the violations described above.
3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;
 - b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. Evidence of the lack of such malicious software;
 - d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.
 - f. Evidence of the times the COMPUTER was used;
 - g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. Records of or information about Internet Protocol addresses used by the COMPUTER;
- j. Records of, or information about, the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. Contextual information necessary to understand the evidence described in this attachment.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of government attorneys and agents is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will review all seized communications and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications with attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team and the investigative team may resume its review. If the filter team decides that any of the communications to/from attorneys are not actually privileged (e.g., the

communication includes a third party or the crime-fraud exception applies), the filter team must obtain a court order before providing these attorney communications to the investigative team.

Your affiant requests the search warrant for the aforementioned items to include the opening and searching of any locked safes, boxes, and compartments.